REMARKS

This amendment is responsive to the non-final Office Action of June 9, 2010. The Office Action has been carefully considered. Applicant requests reconsideration of the claims.

Claims 1-12, 14-15 and 17-24 are pending in this application. Claims 23 and 24 were inadvertently omitted from the list of claims in the previous response. A list of claims that includes these claims is included herein for the sake of completeness. No claims have been added or amended. No amendment to the specification has been made.

REJECTIONS UNDER 35 U.S.C. §103(a)

Claims 1-4, 7-12, 14-15, and 17-20, have been rejected under 35 U.S.C. §103(a) as obvious over the newly-cited U.S. Patent No. 7,203,560 of Wylie et al., in view of the published U.S. Pat. Appln. No. 2008/0186166 of Zhou et al.

The rejection of these claims under 35 U.S.C. 103(a) is hereby respectfully traversed in view of the following remarks.

Unlike Zhou, which was relied upon in previous Office Actions and is principally directed to providing centralized alert services to consumers, Wylie does disclose and discuss some of the problematic characteristics of remote machine control communications in the industrial machine control environment.

In particular, the industrial machine controllers which Wylie describes are clearly computers that are located with the particular respective industrial machines that they control, even though I/O modules of the controller may not be in the same "rack" as that computer, col. 1, lines 44-48. This is also clearly seen in the German-language disclosures of controllers that send emails, etc. that are of record in this application.

However, although Wylie also provides a terminal that allows technicians to maintain and supervise multiple industrial controllers from a remote location, col. 1, line 15 to col. 3, line 55, Wylie neither discloses nor suggests the problem that is addressed by applicant's invention, the problem of providing secure communications between industrial machine controllers and roving technicians. Roving technicians do not work out of a fixed office location. Roving technicians are most often remote from at least some of the controllers that they are responsible for, and/or also remote from the location of their office.

From col. 4, line 45, to col. 5, line 2, Wylie suggests the use of Internet email as well as other both public and private (proprietary) wireless and hardwired communications modalities to communicate with that remote location mentioned in Wylie, without regard for the serious security vulnerability of those public systems, or whether or not the messages will be displayed on a secure terminal. Wylie takes the security of the messages sent by these industrial controllers to the technicians responsible for those controllers for granted. Wylie's disclosure is, instead, directed to improved diagnostic algorithms.

As seen in the German-language disclosures mentioned above, industrial controllers that are known in the art do automatically generate voice and email communications. The automated voice and e-mail messages generated by the conventional industrial controllers, including those noted in the Office Action, rely on private networks and/or PKI encryption for securing email that they send over public networks. However, PKI encryption is not suitable for use by roving technicians when they are away from their office, as is explained in paragraphs [0006] to [0007] of applicant's specification, and the private networks often aren't available to roving technicians, particularly while traveling.

Like those conventional industrial controllers, Wylie, in col. 5, lines 60-65, and col. 8, lines 30-53, simply sends alarm event data to remote users, without regard for whether or not they are in their office or traveling. However, as explained above, technicians in the field can't rely on PKI encryption. Thus, Wylie's communications are either vulnerable to misdirection, and/or interception over the public telephone and data networks that roving technicians rely on when they are out of contact with both their employer's private network and their office or, if those messages are PKI encrypted, they can only be decrypted at the office.

Wylie provides no basis for the proposed combination of Wylie with Zhou. Wylie does not even disclose or suggest the problems in the industrial control environment that could make such a combination advantageous. Thus the proposed combination is purely the product of hindsight, that is, it requires applicant's disclosure of the problem to motivate finding the claimed solution for that problem in a second disclosure.

A combination motivated by hindsight is improper. Therefore this combination of Wylie and Zhou does not support this rejection, which should be withdrawn.

Like the industrial control system disclosed by Wylie, the communication system disclosed by Zhou is designed to send event-relevant information to a fixed central remote location, which in Zhou is the centralized log and alarm service bureau (ASP) seen in Fig. 1. The problem of providing direct communication between a roving technician and multiple remote log and alarm units does not arise in the centralized log and alarm system disclosed by Zhou. Zhou also teaches away from applicant's claimed invention.

As described in Wylie, and in paragraph [0003] of the applicant's specification, industrial machine controllers are located on-site with the machines they control. These industrial machine controllers provide technicians direct access to event-relevant information to the technician on site at the machine's location, whether or not they have a remote connection. These industrial controllers provide the technicians direct access so that the technicians can perform inspection and maintenance work on-site at the machine's location, as is well known in the art. Preferably, roving technicians responding to an alarm while at a remote location should be provided the same secure access to the information as the controller will provide to them when they are physically on-site with the machine and looking directly at its controller.

Although Zhou does suggest providing tracking and monitoring of commercial food (Fig. 11) and hazardous waste (Fig. 13) shipments, and also monitoring of landfill conditions (Fig. 13), even controlling irrigation systems (Fig. 15), Zhou teaches that it all should be done from the same remote location rather than onsite. Even the irrigation valves are controlled by that same remote, multipurpose ASP, not by an industrial irrigation controller, and Zhou's irrigation control alarm is also generated by the ASP [0215] – [0218],

Applicant's secure, direct link between the industrial machine controller itself and the roving technician responsible or that machine is important to industrial safety because it provides a very valuable, redundant access channel for the technician to that controller, because the technician is alerted directly, independent of the remote link to the office that is provided by conventional industrial controllers and also without relying on an ASP. or the office staff, to forward the alert to the technician. This is especially important when storms, floods or accidents damage the communications infrastructure. In contrast, Zhou's ASP requires multiple remote communication links to all be available. Therefore, Zhou's ASP is very vulnerable to disruption.

In contrast, Zhou discloses that the remote service bureau (ASP) is advantageous because it can generate alert messages based on sensed changes in location, as well as parameters monitored from fixed locations [0005]. However, although Zhou's remote ASP may be acceptable for "quasi-industrial" control of this limited kind, and advantageous because it can monitor so many different things, that is, because it is non-specialized and is at a fixed location that is remote from all of them, it is inapposite to applicant's claimed invention and unusable for industrial machine control applications.

However, applicant's industrial machines -- machine tools, robots, processing machines, etc. [0003] - [0005] -- are all already locally monitored and alarmed by their industrial machine controllers, as is well known in the art. Specifically, applicant's claims 1 and 11 recite that the alarm event-relevant information is written to the particular industrial machine's industrial machine controller, which is located with its machine, rather than being written to the remote, multipurpose service bureau disclosed by Zhou which then generates alerts at appropriate times and forwards those alerts to a remote user.

Industrial machine controllers are not general-purpose devices, such as Zhou's ASP. Because of the complexity of automated industrial equipment, each controller can only operate particular types of machines among the various machine tools, robots, processing machines, etc. described in paragraphs [0003] - [0005]. These particular types of controllers for particular types of machines also cannot be remote from the machines they control. Specifically, the industrial controllers must be located on site with the machines that they control, so as to permit inspection and maintenance of those machines. For effective inspection and maintenance of the machines, the operational and alarm event-relevant information that their controllers provide is, necessarily, the most up to date and complete information that can be obtained without taking the machine down and physically inspecting the machine's condition in detail, as is well known in the art.

Since applicant's invention is directed to securely communicating the log and alarm information that industrial controllers already directly provide to the technicians when the technicians are on the company's secure shop floor, Zhou's ASP is both superfluous and inoperative in combination with the conventional industrial machine controllers that are known in the art, and discussed by Wylie. Zhou's disclosure is inapposite to applicant's invention.

Furthermore, Zhou's disclosure also explicitly teaches away from writing the event-relevant information about an alarm event occurring in an industrial machine to its controller, which is a computer located with the machine. On the contrary, Zhou argues that performing both the monitoring and alarm functions and the message generation functions at Zhou's remote, centralized ASP is advantageous because the ASP can then monitor so many different things all from a single, fixed location that is remote from all of them, thereby providing efficient operation and economies of scale. Therefore Zhou cannot suggest communication method suitable for use in the field by a roving technician to receive alarm event information from an industrial machine controller, as recited in applicant's claims.

Zhou, like Wylie, neither discloses nor suggests the security problems of highly automated industrial machines, nor the other problems of providing information from industrial machine controllers to the roving technicians who need it. Furthermore, Zhou neither discloses nor suggests the communication method recited in applicant's claims.

With particular regard to the rejection of claim 11, it seems to assert that that the "secure connections" disclosed by Wylie and Zhou physically "include" the modem connection recited in this claim, which is misleading. However, as best understood, this means that the rejection of claim 11 is once again based on the "same rationale" as that of claim 1. Therefore, it is traversed for the same reason as given above for the rejection of claim 1.

Withdrawal of the rejection of these claims under 35 U.S.C. §103(a) and allowance thereof are thus respectfully requested.

Claim 5 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Wylie in view of Zhou et al., further in view of Qi et al. (US 6892064). This claim depends indirectly from claim 1. Therefore it contains all the limitations thereof and those limitations patentably distinguish this claim over the applied prior art in the same manner as claim 1.

This rejection is therefore hereby respectfully traversed for the reasons given above with respect to the rejection of claim 1 over Wylie and Zhou, et al.

Withdrawal of the rejection of claim 5 under 35 U.S.C. §103(a) and allowance thereof are respectfully requested.

Claim 6 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Wylie in view of Zhou et al., further in view of published U.S. Pat. Appln. No 2007/0208697 of Subramaniam et al. This claim depends directly from claim 1. Therefore it contains all the limitations thereof and those limitations patentably distinguish this claim over the applied prior art in the same manner as claim 1.

This rejection is therefore hereby respectfully traversed for the reasons given above with respect to the rejection of claim 1 over Wylie and Zhou, et al.

Withdrawal of the rejection of claim 6 under 35 U.S.C. §103(a) and allowance thereof are respectfully requested.

CONCLUSION

In view of the above, each of the presently pending claims in this application is considered patentably differentiated over the prior art of record and believed to be in immediate conditions for allowance. Reconsideration and allowance of the present application are thus respectfully requested.

Should the Examiner consider necessary or desirable any formal changes anywhere in the specification, claims and/or drawing, then it is respectfully requested that such changes be made by Examiner's Amendment, if the Examiner feels this would facilitate passage of the case to issuance. If the Examiner feels that it might be helpful in advancing this case by calling the undersigned, applicant would greatly appreciate such a telephone interview.

Respectfully submitted,

By: ______________________

Henry M. Feiereisen
Agent For Applicant
Reg. No: 31,084

Date: October 7, 2010
708 Third Avenue
Suite 1501
New York, N.Y. 10017
(212) 244-5500
HMF/RL:af